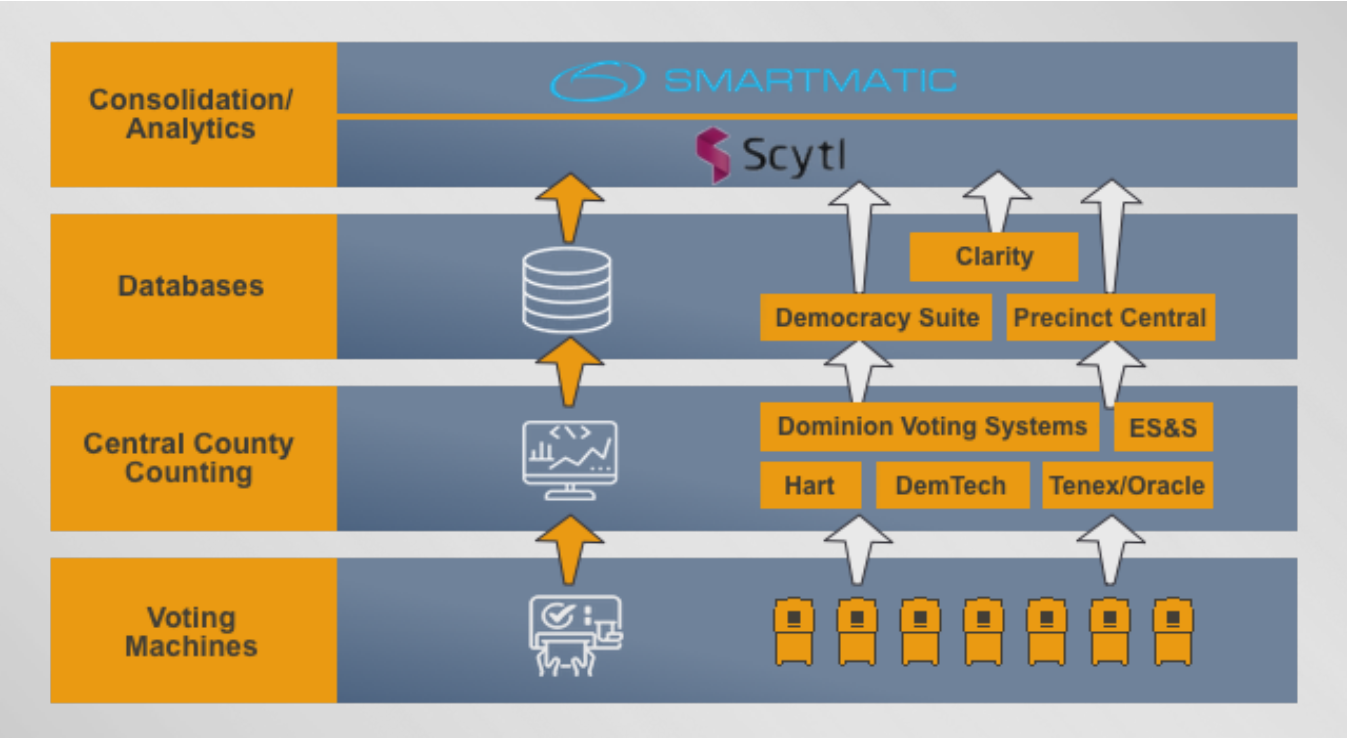
Um Servidor Espanhol

Sobre a Scytl e um computador eleitoral em Frankfurt

#Scytl #SmartMatic #Elections #Fraud

Mqualquer um está familiarizado com os eventos de Torrero na Espanha, nos quais um homem geralmente corajoso entra em uma arena para se envolver diretamente com um touro. Equipado apenas com um tecido vermelho, o Torrero consegue deixar o touro totalmente exausto, permitindo-lhe colocar armas letais no pescoço do touro depois de muitas horas. Quase nos lembramos de tal espetáculo quando um congressista dos EUA insinuou, em meados de novembro de 2020, que alguém na Alemanha espalhou a mensagem de que o Exército dos EUA supostamente confiscou um servidor de computador na capital bancária alemã Frankfurt em 9 de novembro de 2020, ou obteve pelo menos digitalmente todo o seu conteúdo. O servidor pertencia originalmente a uma empresa chamada Scytl, com sede em Barcelona, Espanha. Agora nas mãos de um banco, o servidor de Frankfurt estava supostamente conectado a vários bancos de dados de resultados eleitorais dos EUA 2020, administrados e operados pela Scytl, que entrou com pedido de concordata no verão de 2020 e estava prestes a entrar no processo de liquidação final.

A maioria dos condados estaduais dos EUA usa máquinas de votação para contar milhões de cédulas e alguns sistemas de software importantes para reunir os resultados eletrônicos enviados por essas máquinas. O software mais amplamente utilizado pela grande maioria dos condados dos Estados Unidos são Dominion Voting Systems, Tenex, ES&S, Hart ou DemTech. Depois de receber as cédulas do condado, os vários sistemas de software encaminham as contagens de votos e informações para um punhado de bancos de dados, executados na infraestrutura de TI em nuvem da Amazon AWS e denominados Clarity, Democracy Suite, Delegacia Central. Embora o banco de dados do Clarity seja inteiramente de propriedade da Scytl, os outros são operados ou pelo menos acessíveis pela empresa espanhola.



A empresa, localizada no centro da cidade de Barcelona, a capital catalã, tem uma história interessante que vale a pena contar. Foi fundada em 2001 pelos pesquisadores de sistemas de votação eletrônica Andreu Riera e Carles Rovira, da Universidade de Barcelona, logo após o estouro da bolha das pontocom. Os dois escolheram cuidadosamente o nome da empresa como uma criptografia do primeiro método de criptografia conhecido chamado Skytale, usado para fins militares na Grécia antiga há cerca de 2500 anos. Pere Valles ingressou na empresa desde o início, assim como um grupo financeiro local. Em 2006, o fundador Riera morreu em um acidente de carro. Alguns anos depois, a Nauta Capital tornou-se acionista e, em 2010, a Scytl pagou US $ 10 milhões pela empresa americana SOE Software, um importante fornecedor de soluções de gerenciamento elétrico. As vendas chegaram a 25 milhões de dólares, a empresa tinha escritórios em Washington, DC, Toronto, Nova Delhi, Atenas, Kiev e Cingapura e uma força de trabalho de mais de 400 pessoas. Em 2013, o cofundador da Microsoft Paul Allen investiu 40 milhões de dólares por meio de seu famoso Fundo Vulcan Capital.

Estranhamente, no entanto, apesar dos planos de alistar a empresa na NASDAQ, a fama de Scytl diminuiu nos anos seguintes. As razões são pelo menos duvidosas: projetos falharam e estranhos esforços reorganizacionais estavam sabotando o sucesso projetado de Scytl. Em dezembro de 2019, a empresa entrou com um processo de pré-falência, um tribunal espanhol declarou o fim formal e legal da empresa de Barcelona em 2 de junho de 2020. Anteriormente, os acionistas da Scytl JB Capital, Vulcan Capital, Nauta Capital e Spinnaker conseguiram convencer o fundo americano Sandton Capital para assumir o processo de falência e, aparentemente, Sandton Capital não hesitou muito em reconectar um dos servidores da Scytl em Frankfurt de volta à Internet. Ou veio o pedido do novo dono da Scytl, Paragon Group, que comprou os negócios da Scytl em 20 de outubro de 2020, coincidentemente exatamente 14 dias antes da eleição presidencial dos EUA ?

Outra empresa que se dedica à contagem global de votos é a SGO Smartmatic , em 2014 re-formada como uma empresa do Reino Unido sob o presidente Mark Malloch-Brown. Conectado a George Soros por ter sido o vice-presidente do Quantum Fund do bilionário - agora denominado Open Society Global - Sir Malloch-Brown está profundamente ligado à ONU, aos Clintons e outras organizações Soros. A Smartmatic foi examinada em 2005, quando comprou uma empresa americana chamada Sequoia Voting Systems. Os congressistas norte-americanos solicitaram ao Comitê de Investimento Estrangeiro nos Estados Unidos (CFIUS) que analisasse o negócio já naquela época, uma vez que a Sequoia teria ligações com o governo venezuelano. Autoridades dos EUA declararam em 2006que "parece ter havido um esforço óbvio para obscurecer a propriedade da empresa", referindo-se à rede oculta de fundos e trustes da Smartmatic que participam da empresa do Reino Unido.

Em 2017, a eleição geral venezuelana foi fraudada em cerca de 1 milhão de votos, administrada pelo software Smartmatic, que está em contato com o governo venezuelano desde 2004. Um total de 8 milhões de pessoas votaram nessa eleição, a que se referiu o CEO da Smartmatic, Antonio Mugicana frente de uma assessoria de imprensa em Londres, afirmando que “sabemos, sem dúvida, que o comparecimento da recente eleição para uma Assembleia Nacional Constituinte [da Venezuela] foi manipulado”. Um denunciante afirmou em 2020 que a Smartmatic usa o mesmo software que Dominion Voting Systems, este último sendo usado em quase 30 estados dos EUA, e que o software foi fundamental no passado para manter Hugo Chávez no poder na Venezuela:

Em 2019, um grupo internacional de pesquisadores de fraude eleitoral na Suíça descobriu que o software da Scytl poderia ser facilmente manipulado. Os auditores de software descobriram que uma falha de backdoor no sistema permitiu que cédulas legítimas fossem inteiramente substituídas por votos fraudulentos:

> A vulnerabilidade é surpreendente. Em eleições normais, não há uma única pessoa que possa defraudar indetectavelmente toda a eleição. Mas neste sistema que eles construíram, há um partido que poderia fazer isso. (Matthew Green, professor de criptografia na Universidade Johns Hopkins)

Scytl foi rápido em minimizar a vulnerabilidade de segurança, afirmando que os hackers precisavam de acesso à infraestrutura de TI do Swiss Post, que comprou os direitos do código-fonte do software da Scytl em abril de 2019. A alegação foi que "ajuda de vários insiders com conhecimento especializado de Swiss Post ou os cantões" eram necessários, ignorando ao mesmo tempo o fato de que o grupo de especialistas em segurança não tinha esse acesso ao detectar o problema de software rapidamente.

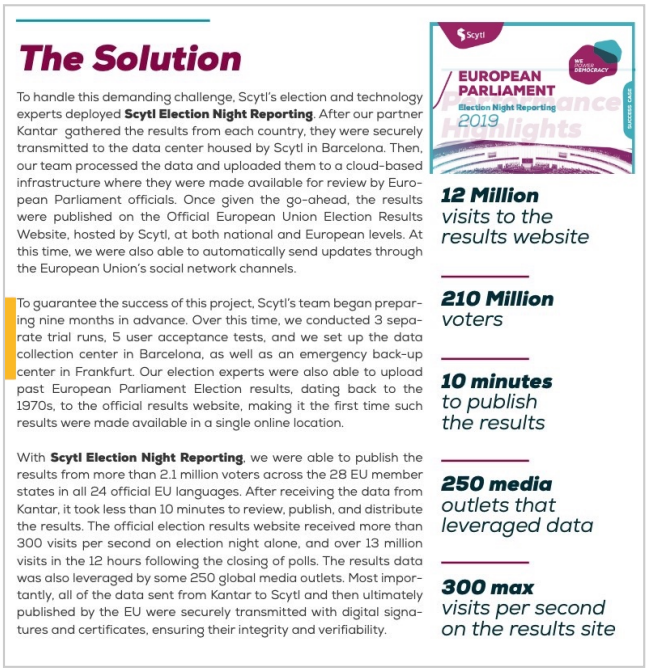
Um incidente semelhante aconteceu após o evento eleitoral torrero US 2020, quando a Scytl foi rápida em desmascarar qualquer alegação de fraude maciça, também em seu servidor em Frankfurt. Um relatório confidencial sobre irregularidades eleitorais, conduzido nos meses que antecedem as eleições presidenciais dos EUA de 2020, no entanto, afirma que os dados das eleições foram encaminhados para

vários servidores fora dos EUA, explicitamente também para um servidor de propriedade da empresa de Barcelona:

> Os registros de votação para as eleições gerais de 2018 foram encaminhados automaticamente do site clarityelections.com para vários endereços DNS nacionais e estrangeiros, incluindo ES&S, Scytl em Barcelona, Smartmatic em Londres e um servidor russo na South Ural State University em Chalyabinsk, um GRU conhecido instalação.
>
> (Relatório resumido sobre irregularidades eleitorais de agosto de 2020)

A própria Scytl deu a entender em 2019 que está ligada à cidade alemã de Frankfurt, apesar de sua afirmação de 2020 "não temos servidores ou escritórios em Frankfurt". A empresa foi selecionada para fornecer a infraestrutura de TI para as eleições europeias de 2019 também. Em um estudo de caso da Scytl de 2019, a empresa afirmou o seguinte:

> Para garantir o sucesso deste projeto [Eleições UE 2019], a equipe da Scytl começou a se preparar com nove meses de antecedência. Ao longo desse tempo, conduzimos 3 execuções de teste separadas, 5 testes de aceitação do usuário e montamos o centro de coleta de dados em Barcelona, bem como um centro de backup de emergência em Frankfurt.
>
> (Estudo de caso de sucesso da Scytl para as eleições da UE 2019, página 3)



The Solution

To handle this demanding challenge, Scytl's election and technology experts deployed **Scytl Election Night Reporting**. After our partner Kantar gathered the results from each country, they were securely transmitted to the data center housed by Scytl in Barcelona. Then, our team processed the data and uploaded them to a cloud-based infrastructure where they were made available for review by European Parliament officials. Once given the go-ahead, the results were published on the Official European Union Election Results Website, hosted by Scytl, at both national and European levels. At this time, we were also able to automatically send updates through the European Union's social network channels.

To guarantee the success of this project, Scytl's team began preparing nine months in advance. Over this time, we conducted 3 separate trial runs, 5 user acceptance tests, and we set up the data collection center in Barcelona, as well as an emergency back-up center in Frankfurt. Our election experts were also able to upload past European Parliament Election results, dating back to the 1970s, to the official results website, making it the first time such results were made available in a single online location.

With **Scytl Election Night Reporting**, we were able to publish the results from more than 2.1 million voters across the 28 EU member states in all 24 official EU languages. After receiving the data from Kantar, it took less than 10 minutes to review, publish, and distribute the results. The official election results website received more than 300 visits per second on election night alone, and over 13 million visits in the 12 hours following the closing of polls. The results data was also leveraged by some 250 global media outlets. Most importantly, all of the data sent from Kantar to Scytl and then ultimately published by the EU were securely transmitted with digital signatures and certificates, ensuring their integrity and verifiability.

Não muito diferente dos eventos de torrero espanhóis, onde geralmente, no final, o touro era arrastado pelas ruas para exibição pública e, portanto, todos para ver.

https://www.sun24.news/pt/um-servidor-espanhol-sobre-a-scytl-e-um-computador-eleitoral-em-frankfurt.html